PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-282982
(43)Date of publication of application : 15.10.1999

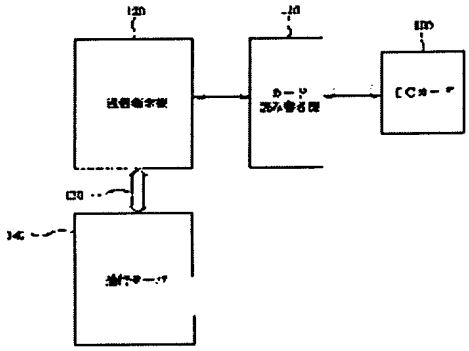
(51)Int.Cl. G06K 17/00
G06F 15/00
G06K 19/10
G06K 19/073
G09C 1/00
H04L 9/10
H04L 9/32

(21)Application number : 10-085536
(22)Date of filing : 31.03.1998

(71)Applicant : OKI ELECTRIC IND CO LTD
(72)Inventor : NISHIYAMA YOSHITAKA

(54) USER CARD, COMMUNICATION TERMINAL EQUIPMENT, COMMUNICATION SERVER, COMMUNICATION SYSTEM AND USER AUTHENTICATION METHOD FOR COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED : To provide a user authentication method of a communication system capable of simplifying the operation of a user and simultaneously authenticating both of the user and a terminal equipment.
SOLUTION : When the user inputs a password for a card to the terminal equipment 120, the terminal equipment 120 transmits a connection request including a terminal equipment ID to a communication network 130 and a server 140 confirms the validity/invalidity of the terminal equipment 120 from the terminal equipment ID and then returns a challenge. Then, the terminal equipment 120 calculates a one-time password by using a seed inside the challenge, a password number and a terminal password and sends it to an IC card 100 together with the password for the card and a random number. The IC card 100 checks the password for the card, then ciphers data including the one-time password and the random number and sends them through the terminal equipment 120 to the server 140. The server 140 deciphers the received data and then, checks the terminal password, the random number and the one-time password.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－282982

(43)公開日　平成11年(1999)10月15日

(51)Int.Cl.⁶	識別記号	ＦＩ	
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｔ
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｇ
			３３０Ｅ
Ｇ０６Ｋ　19/10		Ｇ０９Ｃ　1/00	６６０Ａ
19/073		Ｇ０６Ｋ　19/00	Ｒ

審査請求　未請求　請求項の数17　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願平10－85536

(22)出願日　平成10年(1998)３月31日

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号

(72)発明者　西山　由高
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内

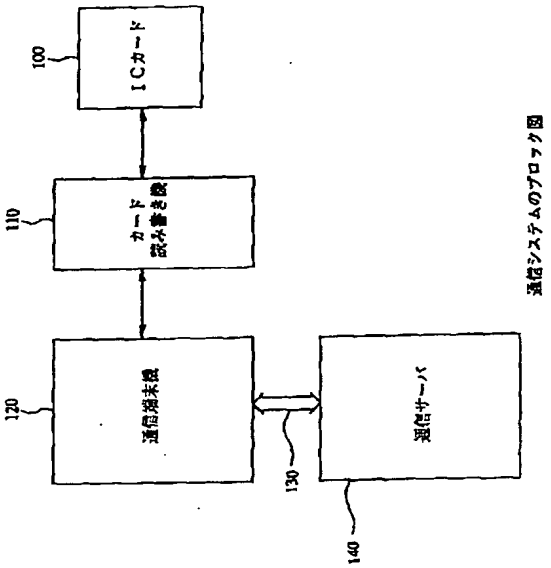
(74)代理人　弁理士　大垣　孝

(54)【発明の名称】　利用者カード、通信端末機、通信サーバ、通信システム、および、通信システムの利用者認証方法

(57)【要約】

【課題】　利用者の操作が簡単で、且つ、利用者と端末機の認証とを両方同時に行うことができる、通信システムの利用者認証方法を提供する。

【解決手段】　端末機１２０に利用者がカード用パスワードを入力すると、この端末機１２０が端末機ＩＤを含む接続要求を通信網１３０に送信し、サーバ１４０が端末機ＩＤから端末機１２０の有効／無効を確認した後、チャレンジを返信する。続いて、端末機１２０が、チャレンジ内のシードおよびパスワード番号と端末パスワードとを用いてワンタイム・パスワードを算出し、カード用パスワードおよび乱数とともにＩＣカード１００に送る。ＩＣカード１００は、カード用パスワードをチャックした後、ワンタイム・パスワードと乱数とを含むデータを暗号化し、端末機１２０を介してサーバ１４０に送る。サーバ１４０は、受信したデータを復号化した後、端末パスワード、乱数およびワンタイム・パスワードのチェックを行う。



通信システムのブロック図

1

【特許請求の範囲】

【請求項１】　利用者が通信網を介して通信端末機と通信サーバとを接続するときの認証を行うための利用者カードであって、

利用者ＩＤ格納領域、カード用パスワード格納領域および秘密鍵格納領域を有する記憶手段と、

外部からカード用パスワードおよび暗号用データを入力し、前記カード用パスワードが前記カード用パスワード格納領域から読み出したパスワードと一致する場合に、前記利用者ＩＤ記憶領域から読み出した利用者ＩＤと前記暗号用データとを連結してなるデータを前記秘密鍵格納領域から読み出した秘密鍵を用いての利用者認証方法暗号化することによりカード暗号文を生成し、このカード暗号文を外部に出力する暗号化手段と、

を備えたことを特徴とする利用者カード。

【請求項２】　前記記憶手段が前記利用者カード内に設けられた不揮発性メモリであることを特徴とする請求項１に記載の利用者カード。

【請求項３】　外部からのカード用パスワードおよび暗号用データの入力と、外部へのカード暗号文の出力とが、カード読み書き装置によって行われることを特徴とする請求項１または２に記載の利用者カード。

【請求項４】　利用者が通信網を介して通信サーバと接続するときに利用者カードを用いて認証を行うための通信端末機であって、

端末機ＩＤ格納領域および端末機用パスワード格納領域を有する記憶手段と、

端末機ＩＤを含む接続要求を前記通信網に送信するとともに、シードとパスワード番号と乱数とを含むチャレンジとを前記通信網から受信するチャレンジ要求手段と、

このチャレンジ要求機能部から取り込んだ前記シードおよび前記パスワード番号と、前記端末機用パスワード格納領域から取り込んだ端末機用パスワードとを用いてワンタイム・パスワードを算出するパスワード生成手段と、

このパスワード生成手段から取り込んだ前記ワンタイムパスワードと前記チャレンジ要求手段から取り込んだ前記乱数とを連結して暗号用データを作成し、この暗号用データと利用者が入力したカード用パスワードとを前記利用者カードに送信するとともに、この利用者カードからカード暗号文を受信する暗号化要求手段と、

この暗号化要求手段から取り込んだ前記カード暗号文を前記通信網に送信するとともに、この通信網から認証結果を受信する認証要求手段と、

を備えたことを特徴とする通信端末機。

【請求項５】　前記利用者カードへの前記暗号用データおよび前記カード用パスワードの送信と、前記利用者カードからの前記カード暗号文の受信とが、カード読み書き装置を介して行われることを特徴とする請求項４に記載の通信端末機。

2

【請求項６】　通信網を介して通信端末機と接続するときに利用者カードを用いて認証を行う通信サーバであって、

シードを記憶するシード記憶手段と、

秘密鍵を記憶する秘密鍵記憶手段と、

端末機ＩＤ、端末機有効／無効情報、パスワード番号および前回の認証時に使用されたワンタイム・パスワードを全ての登録通信端末機について記憶する端末機表と、

利用者ＩＤおよび利用者カード有効／無効情報を全ての登録利用者について記憶する利用者カード表と、

端末機ＩＤを含む接続要求を前記通信網から受信したときに、この端末機ＩＤに対応する端末機有効／無効情報を前記端末機表から読み出し、この端末機有効／無効情報が有効である場合に、前記シード記憶手段から読み出した前記シードと前記端末機表から読み出した前記パスワード番号と新たに生成した乱数とからなるチャレンジを前記通信網に送信するチャレンジ生成手段と、

カード暗号文を受信し、前記秘密鍵記憶手段から読み出した前記秘密鍵で前記カード暗号文を解読することにより利用者ＩＤと乱数とワンタイム・パスワードとを取得し、この利用者ＩＤに対応する前記利用者カード有効／無効情報の有効／無効と、この乱数と前記チャレンジとして送信した前記乱数との一致／不一致とを検証するカード暗号文検証手段と、

このカード暗号文検証手段が取得したワンタイム・パスワードを用いて前回の認証で使用されたワンタイム・パスワードを算出した後、このワンタイム・パスワードを前記端末機表から読みだした前記ワンタイム・パスワードと比較し、両者が一致する場合に、前記カード暗号文検証手段が取得したワンタイム・パスワードを前記端末機表に格納するとともに、この端末機表に記憶されている前記パスワード番号の値を「１」だけ増加させるパスワード検証手段と、

を備えたことを特徴とする通信サーバ。

【請求項７】　前記利用者カードが有効で且つ前記乱数が一致すると前記カード暗号文検証手段が判断し、前記パスワードが一致すると前記パスワード認証手段が判断した場合に、前記通信網に認証応答を出力する認証手段をさらに備えたことを特徴とする請求項６に記載の通信サーバ。

【請求項８】　前記端末機が無効であると前記チャレンジ生成手段が判断した場合、前記利用者カードが無効或いは前記乱数が一致しないと前記カード暗号文検証手段が判断した場合または前記パスワードが一致しないと前記パスワード認証手段が判断した場合に、前記通信端末機との接続を切断することを特徴とする請求項６または７に記載の通信サーバ。

【請求項９】　接続時に認証を行う通信システムであって、

利用者ＩＤ格納領域、カード用パスワード格納領域およ

び秘密鍵格納領域を有するカード用記憶手段と、外部からカード用パスワードおよび暗号用データを入力し、前記カード用パスワードが前記カード用パスワード格納領域から読み出したパスワードと一致する場合に、前記利用者ＩＤ格納領域から読み出した利用者ＩＤと前記暗号用データとを連結してなるデータを前記秘密鍵格納領域から読み出した秘密鍵を用いて暗号化することによりカード暗号文を生成し、このカード暗号文を外部に出力する暗号化手段とを備えた利用者カードと、

端末機ＩＤ格納領域および端末機用パスワード格納領域を有する端末機用記憶手段と、端末機ＩＤを含む接続要求を前記通信網に送信するとともに、シードとパスワード番号と乱数とを含むチャレンジとを前記通信網から受信するチャレンジ要求手段と、このチャレンジ要求機能部から取り込んだ前記シードおよび前記パスワード番号と、前記端末機用パスワード格納領域から取り込んだ端末機用パスワードとを用いてワンタイム・パスワードを算出する端末パスワード生成手段と、このパスワード生成手段から取り込んだ前記ワンタイム・パスワードと前記チャレンジ要求手段から取り込んだ前記乱数とを連結して暗号用データを作成し、この暗号用データと利用者が入力したカード用パスワードとを前記利用者カードに送信するとともに、この利用者カードからカード暗号文を受信する暗号化要求手段と、この暗号化要求手段から取り込んだ前記カード暗号文を前記通信網に送信するとともに、この通信網から認証結果を受信する認証要求手段とを備えた通信端末機と、

シードを記憶するシード記憶手段と、秘密鍵を記憶する秘密鍵記憶手段と、端末機ＩＤ、端末機有効／無効情報、パスワード番号および前回の認証時に使用されたワンタイム・パスワードを全ての登録通信端末機について記憶する端末機表と、利用者ＩＤおよび利用者カード有効／無効情報を全ての登録利用者について記憶する利用者カード表と、端末機ＩＤを含む接続要求を前記通信網から受信したときに、この端末機ＩＤに対応する端末機有効／無効情報を前記端末機表から読み出し、この端末機有効／無効情報が有効である場合に、前記シード記憶手段から読み出した前記シードと前記端末機表から読み出した前記パスワード番号と新たに生成した乱数とからなるチャレンジを前記通信網に送信するチャレンジ生成手段と、カード暗号文を受信し、前記秘密鍵記憶手段から読み出した前記秘密鍵で前記カード暗号文を解読することにより利用者ＩＤと乱数とワンタイム・パスワードとを取得し、この利用者ＩＤに対応する前記利用者カード有効／無効情報の有効／無効と、この乱数と前記チャレンジとして送信した前記乱数との一致／不一致とを検証するカード暗号文検証手段と、このカード暗号文検証手段が取得したワンタイム・パスワードを用いて前回の認証で使用されたワンタイム・パスワードを算出した後、このワンタイム・パスワードを前記端末機表から読みだした前記ワンタイム・パスワードと比較し、両者が一致する場合に、前記カード暗号文検証手段が取得したワンタイム・パスワードを前記端末機表に格納するとともに、この端末機表に記憶されている前記パスワード番号の値を「１」だけ増加させるパスワード検証手段とを備えた通信サーバと、

を有することを特徴とする通信システム。

【請求項１０】　前記カード用記憶手段が前記利用者カード内に設けられた不揮発性メモリであることを特徴とする請求項９に記載の通信システム。

【請求項１１】　外部から利用者カードへのカード用パスワードおよび暗号用データの入力と、利用者カードから外部へのカード暗号文の出力とが、カード読み書き装置によって行われることを特徴とする請求項９または１０に記載の通信システム。

【請求項１２】　前記利用者カードが有効で且つ前記乱数が一致すると前記カード暗号文検証手段が判断し、前記パスワードが一致すると前記パスワード認証手段が判断した場合に、前記通信網に認証応答を出力する認証手段をさらに備えたことを特徴とする請求項９～１１のいずれかに記載の通信システム。

【請求項１３】　前記端末機が無効であると前記チャレンジ生成手段が判断した場合、前記利用者カードが無効或いは前記乱数が一致しないと前記カード暗号文検証手段が判断した場合または前記パスワードが一致しないと前記パスワード認証手段が判断した場合に、前記通信サーバが前記通信端末機との接続を切断することを特徴とする請求項９～１２のいずれかに記載の通信システム。

【請求項１４】　通信網を介して通信端末機と通信サーバとを接続したときに利用者および通信端末機を認証するための、通信システムの利用者認証方法であって、

通信端末機が、端末機ＩＤを含む接続要求を前記通信網に送信する第１過程と、

通信サーバが、前記通信網から前記接続要求を受信して、この接続要求内の前記端末機ＩＤに対応する端末機有効／無効情報が有効である場合に、シード記憶手段に記憶されたシードと端末機表に記憶されたパスワード番号と新たに生成した乱数とからなるチャレンジを前記通信網に送信する第２過程と、

前記通信端末機が、前記チャレンジを前記通信網から受信し、このチャレンジ内の前記シードおよび前記パスワード番号と端末機用パスワードとを用いてワンタイム・パスワードを算出する第３過程と、

前記ワンタイム・パスワードと前記乱数とを連結して暗号用データを作成し、利用者が入力したカード用パスワードとともに、前記通信端末機から利用者カードに転送する第４過程と、

前記利用者カードが、前記カード用パスワードがパスワード格納領域に記憶されたパスワードと一致する場合に、利用者ＩＤ格納領域に記憶された利用者ＩＤと前記

暗号用データとを連結してなるデータを秘密鍵で暗号化することによりカード暗号文を生成し、このカード暗号文を前記通信端末機に送信する第５過程と、
前記通信端末機が前記カード用暗号文を前記通信網に転送する第６過程と、
前記通信サーバが、前記通信網から受信した前記カード用暗号文を秘密鍵で解読することにより利用者ＩＤと乱数とワンタイム・パスワードとを取得し、この利用者ＩＤに対応する利用者カード有効／無効情報の有効／無効と、この乱数と前記チャレンジとして送信した前記乱数との一致／不一致とを検証する第７過程と、
前記カード用暗号文を解読して得られた前記ワンタイム・パスワードを用いて前回の認証で使用されたワンタイム・パスワードを算出した後、このワンタイム・パスワードを前記端末機表に記憶された前回の認証で実際に使用されたワンタイム・パスワードと比較し、両者が一致する場合に、前記カード用暗号文を解読して得られた前記ワンタイム・パスワードを前記端末機表に格納するとともに、この端末機表に記憶されている前記パスワード番号の値を「１」だけ増加させる第８過程と、
を有することを特徴とする通信システムの利用者認証方法。

【請求項１５】　外部からのカード用パスワードおよび暗号用データの入力と、外部へのカード暗号文の出力とが、カード読み書き装置によって行われることを特徴とする請求項１４に記載の通信システムの利用者認証方法。

【請求項１６】　前記利用者カードが有効で且つ前記乱数が一致すると前記第７過程で判断され、前記パスワードが一致すると前記第８過程で判断された場合に、前記通信サーバが前記通信網に認証応答を出力することを特徴とする請求項１４または１５に記載の通信システムの利用者認証方法。

【請求項１７】　前記端末機が無効であると前記第２過程で判断された場合、前記利用者カードが無効或いは前記乱数が一致しないと前記第７過程で判断され場合または前記パスワードが一致しないと前記第８過程で判断された場合に、前記通信サーバが前記通信端末機との接続を切断することを特徴とする請求項１４～１７のいずれかに記載の通信システムの利用者認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、通信網を介して通信端末機と通信サーバとを接続したときに利用者の正当性を検証する技術に関するものである。

【０００２】

【従来の技術】通信網を介して通信端末機と通信サーバとを接続したときには、利用者が接続の権利を有するものであるか否かを確認する必要がある。

【０００３】従来の通信網では、この確認は、利用者が、通信端末を用いて利用者ＩＤとパスワードとを通信サーバに送信することによって、行われていた。

【０００４】このため、他人が利用者からパスワードを盗んで通信網を不正に使用しないための防護策が、必要であった。

【０００５】従来は、パスワードの盗難を防止するために、利用者がパスワードを適宜変更することを可能にしていた。しかし、この方法では、実際には、同一のパスワードが多数回にわたって使用されることが多い。また、一般には、利用者は、盗難が発生したことをすぐには気づかない場合が多い。このため、利用者のパスワードが他人に盗まれた場合には、この利用者がパスワードを変更するまでの間、パスワードを盗んだ他人の不正使用を許してしまうこととなる。

【０００６】パスワードの盗難は、利用者がパスワードの入力作業を他人に見られた場合や、他人が管理する通信端末機等を使用して通信サーバに接続する場合や、ネットワーク上でパスワードをコピーされた場合などに、発生する。

【０００７】これに対して、他人の不正使用を防止できる利用者認証方法として、「ワンタイム・パスワード」を用いた方法が提案されている。この方法を開示した文献としては、例えば、以下のようなものがある。

【０００８】①稲村雄　“ワンタイム・パスワード”　雑誌「オープンデザイン」No. １４１９９６年６月号第３０頁～第３９頁　ＣＱ出版社

②Ravi Kalakota and Andrew B. Whinston, “Token or Smart-Card Authentication”, Frontier of Electronic Commerce , p. 204, Addison-Wesley Publishingcompany, Inc., 1996.

このワンタイム・パスワードを用いた場合、同一のパスワードは一回しか使用されないので、他人がパスワードを盗んで不正に使用することを有効に防止できる。

【０００９】

【発明が解決しようとする課題】上述の文献に開示されているように、ワンタイム・パスワード法では、ワンタイム・パスワードを算出するための関数として、一方向関数Ｆ(x) を用いる。すなわち、このワンタイム・パスワード法では、一方向関数Ｆ(x) を用いて、ｍ－１回目の認証作業で用いたワンタイム・パスワードからｍ回目の認証作業で用いるワンタイム・パスワードを計算することが非常に困難で、且つ、ｍ回目の認証作業で用いたワンタイム・パスワードからｍ－１回目の認証作業で用いたワンタイム・パスワードを計算することは簡単であるような、ワンタイム・パスワード列を作成する。

【００１０】ワンタイム・パスワード生成プログラムは、信頼のおけるコンピュータ上で実行される。利用者は、まず、自分で任意に決定したパスワードとシード（そのサーバに固有の数値を示す文字列）とを、このコンピュータに入力する。

【００１１】ワンタイム・パスワード生成プログラムは、このパスワードとシードとを連結して文字列ｓを作成し、このｓを用いた一方向関数Ｆ(s) の演算を実行する。この一方向関数としては、通信サーバによって定められた関数が使用され、例えばＭＤ４，ＭＤ５，ＳＨＡ１等が使用できる。ここでは、この演算の結果をＰ$_{n}$（すなわち$P_n = F(s)$）とする。

【００１２】続いて、ワンタイム・パスワード生成プログラムは、１回目の演算結果P_nを用いた一方向関数$P_{n-1} = F(P_n)$の演算を実行する。以下同様にして、前回の演算結果を用いた一方向関数の演算を繰り返し実行することにより、下記の演算結果P_x，P_{n-1}，・・・，P_0を得る。これらの演算結果P_n，P_{n-1}，・・・，P_0が、ワンタイム・パスワード列を構成する。

【００１３】

$P_3 = F(s)$
$P_{3-1} = F(P_3)$
$P_{3-2} = F(P_{3-1})$
・
・
・
$P_1 = F(P_2)$
$P_0 = F(P_1)$

次に、利用者が、通信端末機を用いて、利用者名と演算結果P_0とを通信サーバに登録する。そして、利用者は、通信端末機を通信サーバに接続を行う度に、上述の演算結果P_1・・・P_nを、ワンタイム・パスワードとして、P_1から順番に１個ずつ使用していく。

【００１４】一方、通信サーバは、ワンタイム・パスワードP_1を通信端末機から受信すると、このワンタイム・パスワードP_1を用いて$P_0 = F(P_1)$を演算する。続いて、演算結果P_0を、利用者によって先に登録されたP_0と比較する。そして、両者が一致した場合は、ワンタイム・パスワードP_1を次回の認証用データとして記憶するとともに、利用回数として「１」を記憶する。これと同様に、２回目以降の認証（ここではｍ回目とする）においても、通信サーバは、通信端末機から受信したワンタイム・パスワードP_mを用いて$P_{m-1} = F(P_m)$を演算し、この演算結果を前回（すなわちｍ－１回目）のワンタイム・パスワードと比較することにより、利用者の認証を行うことができる。

【００１５】上述したように、ワンタイム・パスワードの演算には、一方向関数Ｆ(x) を使用しているので、ｍ回目のワンタイム・パスワードP_mからｍ－１回目のワンタイム・パスワードP_{m-1}（$= F(P_m)$）を算出することは容易であるが、ｍ回目のワンタイム・パスワードP_mからｍ＋１回目のワンタイム・パスワードP_{m+1}を算出することは困難である。従って、このワンタイム・パスワードを通信端末機から通信サーバに送信する際に他人に盗まれても、盗んだパスワードを用いて他人が通信サーバに不正にログインすることは非常に困難である。また、利用者の秘密のパスワードを通信サーバに送信する必要はないので、この秘密のパスワードを他人に盗まれる可能性も少ない。

【００１６】但し、上述のようにして算出したワンタイム・パスワード列P_n，P_{n-1}，・・・，P_0をそのままコンピュータに記憶させておくと、このコンピュータから他人がワンタイム・パスワードを読み出して不正使用するおそれがある。このため、実際の運用上は、以下のようにして、接続作業のたびに、利用者がワンタイム・パスワードを算出する。

【００１７】まず、利用者が利用者ＩＤを通信端末機に入力し、この利用者ＩＤと接続要求コードとを通信端末機から通信サーバに送信する。通信サーバは、これらの情報を受信すると、この利用者のパスワード利用回数を示すデータと上述のシードとを、通信端末機に送信する。これらの送信データ全体を「チャレンジ」と称する。なお、ここではｍ回目の接続を行う場合を例にとって説明する。このため、チャレンジに含まれる利用回数データは「ｍ－１」となる。

【００１８】そして、利用者は、予め用意されたパスワード生成プログラムをコンピュータ上で実行する。このプログラムは、シードと利用者の秘密のパスワードとを用いて文字列ｓを作成した後、上述の一方向関数$P_n = F(s)$，$P_{n-1} = F(P_n)$，・・・$P_m = F(P_{m+1})$の演算を順次実行する。これにより、今回の接続（すなわちｍ回目の接続）で使用されるワンタイム・パスワードP_mを算出することができる。そして、このようにして生成されたワンタイム・パスワードP_mが、通信端末機から通信サーバに送信される。通信サーバは、ワンタイム・パスワードを受信すると、受信したワンタイム・パスワードから前回の接続（すなわちｍ－１回目の接続）で使用したワンタイム・パスワードを演算し、この演算結果をサーバ内に記憶された前回のワンタイム・パスワードと比較する。そして、両者が一致する場合に利用者を正当であると認証する。

【００１９】なお、パスワード生成プログラムは、一般には通信端末機上で実行することができるが、携帯型のパスワード生成機を使用することも可能である。このパスワード生成機を利用することにより、パスワード生成プログラムを実行できない通信端末機で通信を行う場合にもワンタイム・パスワードによる認証方法を用いることができ、また、他人が管理する通信端末機等で通信を行う場合に上述の「利用者の秘密のパスワード」が盗まれることを防止できる。

【００２０】このような方法によれば、同一のパスワードは一回しか使用されないので、利用者がパスワードの入力作業を他人に見られた場合や、ネットワーク上でパスワードをコピーされた場合でも、その他人による不正使用が発生するおそれが少ない。

【００２１】しかしながら、ワンタイム・パスワード法には、使用者がチャレンジと秘密のパスワードとを用いて自分でワンタイム・パスワードを算出しなければならず、このため、接続時の操作が煩雑になるという欠点があった。また、上述のようなパスワード生成機を用いてワンタイム・パスワードを生成する場合には、このパスワード生成機を携帯していなければならず、この点でも利用者の負担が大きかった。

【００２２】また、上述のような方法では、利用者の秘密のパスワードをネットワーク上で他人に盗まれるおそれはないものの、ワンタイム・パスワードの演算を行う際に他人に秘密のパスワードを盗まれた場合には、その他人が自分でワンタイム・パスワードを生成して不正使用を行うことが可能であり、不正使用の防止が不十分であった。

【００２３】さらに、ワンタイム・パスワード法では、利用者の認証のみを行い、通信端末機の認証は行っていなかったので、偽造された通信端末機の使用を防止することができないという欠点があった。偽造された通信端末機を利用者に使用させることにより、例えば第三者が通信サーバから送られてきた情報をコピーして盗むなどの不正を行うことが可能となる。このような不正を防止するためには、通信端末機に対しても認証を行うことが望ましい。

【００２４】加えて、通信サーバによって提供されるサービスの不正使用を防止するためには、利用できるサービスを利用者ごと或いは通信端末機ごとに制限することが望ましい場合がある。例えば、銀行における口座振替のサービスの場合であれば、ＡＴＭ(Automatic Tellers Machine) の要に厳しい管理が行われている端末機では金額や利用回数を制限しないが、ホームバンキング用端末機のように厳しい管理が困難な端末機では１回の口座振替で許可する金額や１日の利用回数を制限するというように、通信端末機の機能や設置場所等に応じてサービス内容に差異を設けることが望ましい。このような点からも、通信サーバによる認証は、利用者と通信端末機との両方について行うことが望ましい。

【００２５】このような理由から、利用者の操作が簡単で、且つ、利用者と通信端末機の認証とを両方行うことができる利用者認証方法が嘱望されていた。

【００２６】

【課題を解決するための手段】

（１）第１の発明は、利用者が通信網を介して通信端末機と通信サーバとを接続するときの認証を行うための利用者カードに関する。

【００２７】そして、利用者ＩＤ格納領域、カード用パスワード格納領域および秘密鍵格納領域を有する記憶手段と、外部からカード用パスワードおよび暗号用データを入力し、カード用パスワードがカード用パスワード格納領域から読み出したパスワードと一致する場合に、利用者ＩＤ格納領域から読み出した利用者ＩＤと暗号用データとを連結してなるデータを秘密鍵格納領域から読み出した秘密鍵を用いて暗号化することによりカード暗号文を生成し、このカード暗号文を外部に出力する暗号化手段とを備える。

【００２８】（２）第２の発明は、利用者が通信網を介して通信サーバと接続するときに利用者カードを用いて認証を行うための通信端末機に関する。

【００２９】そして、端末機ＩＤ格納領域および端末機用パスワード格納領域を有する記憶手段と、端末機ＩＤを含む接続要求を通信網に送信するとともに、シードとパスワード番号と乱数とを含むチャレンジとを通信網から受信するチャレンジ要求手段と、このチャレンジ要求機能部から取り込んだシードおよびパスワード番号と、端末機用パスワード格納領域から取り込んだ端末機用パスワードとを用いてワンタイム・パスワードを算出する端末パスワード生成手段と、このパスワード生成手段から取り込んだワンタイム・パスワードとチャレンジ要求手段から取り込んだ乱数とを連結して暗号用データを作成し、この暗号用データと利用者が入力したカード用パスワードとを利用者カードに送信するとともに、この利用者カードからカード暗号文を受信する暗号化要求手段と、この暗号化要求手段から取り込んだカード暗号文を通信網に送信するとともに、この通信網から認証結果を受信する認証要求手段とを備える。

【００３０】（３）第３の発明は、通信網を介して通信端末機と接続するときに利用者カードを用いて認証を行う通信サーバに関する。

【００３１】そして、シードを記憶するシード記憶手段と、秘密鍵を記憶する秘密鍵記憶手段と、端末機ＩＤ、端末機有効／無効情報、パスワード番号および前回の認証時に使用されたワンタイム・パスワードを全ての登録通信端末機について記憶する端末機表と、利用者ＩＤおよび利用者カード有効／無効情報を全ての登録利用者について記憶する利用者カード表と、端末機ＩＤを含む接続要求を通信網から受信したときに、この端末機ＩＤに対応する端末機有効／無効情報を端末機表から読み出し、この端末機有効／無効情報が有効である場合に、シード記憶手段から読み出したシードと端末機表から読み出したパスワード番号と新たに生成した乱数とからなるチャレンジを通信網に送信するチャレンジ生成手段と、通信網からカード暗号文を受信し、秘密鍵記憶手段から読み出した秘密鍵でカード暗号文を解読することにより利用者ＩＤと乱数とワンタイム・パスワードとを取得し、この利用者ＩＤに対応する利用者カード有効／無効情報の有効／無効と、この乱数とチャレンジとして送信した乱数との一致／不一致とを検証するカード暗号文検証手段と、このカード暗号文検証手段が取得したワンタイム・パスワードを用いて前回の認証で使用されたワンタイム・パスワードを算出した後、このワンタイム・パ

スワードを端末機表から読みだしたワンタイム・パスワードと比較し、両者が一致する場合に、カード暗号文検証手段が取得したワンタイム・パスワードを端末機表に格納するとともに、この端末機表に記憶されているパスワード番号の値を「１」だけ増加させるパスワード検証手段とを備える。

【００３２】（４）第４の発明は、接続時に認証を行う通信システムに関する。

【００３３】そして、利用者ＩＤ格納領域、カード用パスワード格納領域および秘密鍵格納領域を有するカード用記憶手段と、外部からカード用パスワードおよび暗号用データを入力し、カード用パスワードがカード用パスワード格納領域から読み出したパスワードと一致する場合に、利用者ＩＤ格納領域から読み出した利用者ＩＤと暗号用データとを連結してなるデータを秘密鍵格納領域から読み出した秘密鍵を用いて暗号化することによりカード暗号文を生成し、このカード暗号文を外部に出力する暗号化手段とを備えた利用者カードと、端末機ＩＤ格納領域および端末機用パスワード格納領域を有する端末機用記憶手段と、端末機ＩＤを含む接続要求を通信網に送信するとともに、シードとパスワード番号と乱数とを含むチャレンジとを通信網から受信するチャレンジ要求手段と、このチャレンジ要求機能部から取り込んだシードおよびパスワード番号と、端末機用パスワード格納領域から取り込んだ端末機用パスワードとを用いてワンタイム・パスワードを算出する端末パスワード生成手段と、このパスワード生成手段から取り込んだワンタイム・パスワードとチャレンジ要求手段から取り込んだ乱数とを連結して暗号用データを作成し、この暗号用データと利用者が入力したカード用パスワードとを利用者カードに送信するとともに、この利用者カードからカード暗号文を受信する暗号化要求手段と、この暗号化要求手段から取り込んだカード暗号文を通信網に送信するとともに、この通信網から認証結果を受信する認証要求手段とを備えた通信端末機と、シードを記憶するシード記憶手段と、秘密鍵を記憶する秘密鍵記憶手段と、端末機ＩＤ、端末機有効／無効情報、パスワード番号および前回の認証時に使用されたワンタイム・パスワードを全ての登録通信端末機について記憶する端末機表と、利用者ＩＤおよび利用者カード有効／無効情報を全ての登録利用者について記憶する利用者カード表と、端末機ＩＤを含む接続要求を通信網から受信したときに、この端末機ＩＤに対応する端末機有効／無効情報を端末機表から読み出し、この端末機有効／無効情報が有効である場合に、シード記憶手段から読み出したシードと端末機表から読み出したパスワード番号と新たに生成した乱数とからなるチャレンジを通信網に送信するチャレンジ生成手段と、通信網からカード暗号文を受信し、秘密鍵記憶手段から読み出した秘密鍵でカード暗号文を解読することにより利用者ＩＤと乱数とワンタイム・パスワードとを取得し、この利用者ＩＤに対応する利用者カード有効／無効情報の有効／無効と、この乱数とチャレンジとして送信した乱数との一致／不一致とを検証するカード暗号文検証手段と、このカード暗号文検証手段が取得したワンタイム・パスワードを用いて前回の認証で使用されたワンタイム・パスワードを算出した後、このワンタイム・パスワードを端末機表から読みだしたワンタイム・パスワードと比較し、両者が一致する場合に、カード暗号文検証手段が取得したワンタイム・パスワードを端末機表に格納するとともに、この端末機表に記憶されているパスワード番号の値を「１」だけ増加させるパスワード検証手段とを備えた通信サーバとを有する。

【００３４】（５）第５の発明は、通信網を介して通信端末機と通信サーバとを接続したときに利用者および通信端末機を認証するための、通信システムの利用者認証方法に関する。

【００３５】そして、通信端末機が、端末機ＩＤを含む接続要求を通信網に送信する第１過程と、通信サーバが、通信網から接続要求を受信して、この接続要求内の端末機ＩＤに対応する端末機有効／無効情報が有効である場合に、シード記憶手段に記憶されたシードと端末機表に記憶されたパスワード番号と新たに生成した乱数とからなるチャレンジを通信網に送信する第２過程と、通信端末機が、チャレンジを通信網から受信し、このチャレンジ内のシードおよびパスワードと端末機用パスワードとを用いてワンタイム・パスワードを算出する第３過程と、ワンタイム・パスワードと乱数とを連結して暗号用データを作成し、利用者が入力したカード用パスワードとともに、通信端末機から利用者カードに転送する第４過程と、利用者カードが、カード用パスワードがパスワード格納領域に記憶されたパスワードと一致する場合に、利用者ＩＤ格納領域に記憶された利用者ＩＤと暗号用データとを連結してなるデータを秘密鍵で暗号化することによりカード暗号文を生成し、このカード暗号文を通信端末機に送信する第５過程と、通信端末機がカード用暗号文を通信網に転送する第６過程と、通信サーバが、通信網から受信したカード用暗号文を秘密鍵で解読することにより利用者ＩＤと乱数とワンタイム・パスワードとを取得し、この利用者ＩＤに対応する利用者カード有効／無効情報の有効／無効と、この乱数とチャレンジとして送信した乱数との一致／不一致とを検証する第７過程と、カード用暗号文を解読して得られたワンタイム・パスワードを用いて前回の認証で使用されたワンタイム・パスワードを算出した後、このワンタイム・パスワードを端末機表に記憶された前回の認証で実際に使用されたワンタイム・パスワードと比較し、両者が一致する場合に、カード用暗号文を解読して得られたワンタイム・パスワードを端末機表に格納するとともに、この端末機表に記憶されているパスワード番号の値を「１」だけ増加させる第８過程とを有する。

【００３６】（６）この発明によれば、使用者が自分でワンタイム・パスワードを算出する必要がないので、接続時の操作が簡単になり、パスワード生成機を携帯する必要もない。また、カード用パスワードは通信端末機を介して通信サーバに送信されないので、このカード用パスワードを外部から不正に読み出すことはできず、従って、他人が利用者カードの不正使用を行うことは不可能である。さらに、通信サーバが利用者の認証と通信端末機の認証とを同時に行うことができる。

【００３７】

【発明の実施の形態】以下、この発明の実施の形態について、図面を用いて説明する。なお、図中、各構成成分の大きさ、形状および配置関係は、この発明が理解できる程度に概略的に示してあるにすぎず、また、以下に説明する数値的条件は単なる例示にすぎないことを理解されたい。

【００３８】図１は、この実施の形態に係る通信システムの全体構成を概略的に示すブロック図である。また、図２はＩＣカードの内部構成を概略的に示すブロック図、図３は通信端末機の内部構成を概略的に示すブロック図、図４は通信サーバの内部構成を概略的に示すブロック図である。

【００３９】図１において、利用者カードとしてのＩＣカード１００は、カード読み書き機１１０にセットされると、このカード読み書き機１１０を介して通信端末機１２０に接続される。また、通信端末機１２０は、通信網１３０を介して、通信サーバ１４０と接続される。

【００４０】図２に示したＩＣカード１００において、利用者ＩＤ格納領域１０１にはこのＩＣカード１００の利用者名を示す情報である利用者ＩＤ（例えば１０バイト長）が、カード用パスワード格納領域１０２にはこのＩＣカードの使用者を認証するためのカード用パスワード（例えば８バイト長）が、秘密鍵格納領域１０３には所定データ（後述）を暗号化することによりカード暗号文を生成するための秘密鍵（例えばＤＥＳ(Data Encription Standard)方式のもの）が、それぞれ格納される。

【００４１】また、暗号化機能部１０４は、後述のようにして、カード用パスワードのチェックと、カード暗号文の生成とを行う。

【００４２】図３に示した通信端末機１２０において、端末機ＩＤ格納領域１２１にはこの通信端末機１２０を示す情報である端末機ＩＤ（例えば８バイト長）が、端末パスワード格納領域１２２にはこの通信端末機１２０を認証するための端末パスワード（例えば８バイト長）が、それぞれ格納される。

【００４３】チャレンジ要求機能部１２３は、通信網１３０を介して通信サーバ１４０にチャレンジ要求を行うとともに、通信サーバ１４０からチャレンジ（シード、パスワード番号および乱数から構成される）を取得する。

【００４４】パスワード生成機能部１２４は、後述するように、チャレンジ中のシードおよびパスワード番号と端末パスワード格納領域１２２から読み出した端末機パスワードとを用いてワンタイム・パスワード（例えば８バイト長）を生成する。

【００４５】暗号化要求機能部１２５は、パスワード生成機能部１２４が生成したワンタイム・パスワードと、端末パスワード格納領域１２２から読み出した端末パスワードと、チャレンジ中の乱数とを連結してなるデータを、ＩＣカード１００の暗号化機能部１０４に送る。また、この暗号化機能部１０４からカード暗号文を受信する。

【００４６】認証要求機能部１２６は、暗号化要求機能部１２５から取り込んだカード暗号文を通信網１３０に送信するとともに、この通信網１３０から認証結果を受信する。

【００４７】図４に示した通信サーバ１４０において、シード格納領域１４１にはシード（そのサーバに固有の文字列）が、秘密鍵格納領域１４２には秘密鍵が、それぞれ記憶されている。

【００４８】端末機表１４３は、端末機ＩＤ、端末機有効／無効情報、パスワード番号および前回の認証時に使用されたワンタイム・パスワードを全ての登録通信端末機について記憶する。

【００４９】ＩＣカード表１４４は、利用者ＩＤおよびＩＣカード有効／無効情報を全ての登録利用者について記憶する。

【００５０】チャレンジ生成機能部１４５は、通信端末機１２０のチャレンジ要求機能部１２３からチャレンジ要求を受信したときに、この通信端末機１２０の有効／無効の判断を行う。そして、この通信端末機１２０が有効である場合に、シード、パスワード番号および乱数からなるチャレンジを、チャレンジ要求機能部１２３に送信する。

【００５１】カード暗号文検証機能部１４６は、後述の認証機能部１４８から入力したカード暗号文を秘密鍵で解読することにより利用者ＩＤと乱数とワンタイム・パスワードとを取得し、この利用者ＩＤに対応する前記ＩＣカード有効／無効情報の有効／無効と、この乱数と前記チャレンジとして送信した前記乱数との一致／不一致とを検証する。

【００５２】パスワード検証機能部１４７は、カード暗号文検証機能部１４６から入力したワンタイム・パスワードを用いて前回の認証で使用されたワンタイム・パスワードを算出した後、このワンタイム・パスワードを端末機表１４３から読み出したワンタイム・パスワードと比較し、両者が一致する場合に、カード暗号文検証機能部１４６が取得したワンタイム・パスワードを端末機表１４３に格納するとともに、この端末機表１４３に記憶されているパスワード番号の値を「１」だけ増加させ

る。

【００５３】認証機能部１４８は、通信端末機１２０から受信したカード暗号文をカード暗号文検証機能部１４６に転送し、このカード暗号文検証機能部１４６から入力したワンタイム・パスワードをパスワード検証機能部１４７に転送し、さらに、このパスワード検証機能部１４７がワンタイム・パスワードが有効であると判断した場合に、通信網１３０に認証応答を送信する。

【００５４】次に、図１～図４に示した通信システムの全体動作について説明する。

【００５５】まず、利用者が、自分のＩＣカード１００をカード読み書き機１１０にセットする。これにより、このカード読み書き機１１０を介して、ＩＣカード１００と通信端末機１２０とが接続される。

【００５６】続いて、利用者が、図示しない入力装置を用いて、通信端末機１２０の認証要求機能部１２６にカード用パスワードを入力する。

【００５７】通信端末機１２０の認証要求機能部１２６は、利用者によってカード用パスワードが入力されると、チャレンジ要求機能部１２３を起動する。このチャレンジ要求機能部１２３は、端末機ＩＤ格納領域１２１から端末機ＩＤを読み出して、この端末機ＩＤを含むチャレンジ要求を通信網１３０に出力する。

【００５８】このチャレンジ要求は、通信網１３０を介して、通信サーバ１４０のチャレンジ生成機能部１４５に受信される。チャレンジ生成機能部１４５は、チャレンジ要求を受信すると、まず、このチャレンジ要求に含まれる端末機ＩＤに対応する端末機有効／無効情報を端末機表から読み出す。そして、この端末機有効／無効情報が「有効」である場合には、チャレンジ生成機能部１４５は、シード格納領域１４１からのシードの読み出しと端末機表１４３からのパスワード番号の読み出しとを行い、さらに、このチャレンジ生成機能部１４５内で乱数を生成する。その後、このチャレンジ生成機能部１４５は、かかるシード、パスワード番号および乱数からチャレンジを生成して、通信網１３０に出力する。一方、端末機有効／無効情報が「無効」である場合には、通信サーバ１４０は、所定の異常処理を行って回線を切断する。

【００５９】チャレンジ要求機能部１２３は、通信網１３０からチャレンジを受信すると、このチャレンジに含まれるシード、パスワード番号および乱数を、認証要求機能部１２６に送る。

【００６０】認証要求機能部１２６は、かかるシード、パスワード番号および乱数のうち、シードおよびパスワード番号を、パスワード生成機能部１２４に送る。

【００６１】パスワード生成機能部１２４は、シードおよびパスワード番号（ここでは「m」とする）を受信すると、続いて、端末パスワード格納領域１２２から端末機パスワードを読み出す。そして、シードと端末パスワードとを用いて文字列ｓを作成した後、従来と同様の一方向関数$P_1 = F(s)$，$P_{i+1} = F(P_i)$，・・・$P_m = F(P_{m-1})$の演算を順次実行する。ここで、一方向関数としては、従来と同様、例えばＭＤ４，ＭＤ５，ＳＨＡ１等が使用できる。さらに、パスワード生成機能部１２４は、演算結果P_m（ここでは１６バイトとする）の上位８バイトと下位８バイトの排他的論理和を演算する。そして、この演算の結果が、ワンタイム・パスワードとして、パスワード生成機能部１２４から認証要求機能部１２６に送られる。

【００６２】認証要求機能部１２６は、このワンタイム・パスワードと、利用者が入力したカード用パスワード（上述）と、チャレンジ要求機能部１２３から受信した乱数（上述）とを、暗号化要求機能部１２５に送る。

【００６３】暗号化要求機能部１２５は、ワンタイム・パスワードと乱数とを連結してなる暗号用データを生成し、この暗号用データをカード用パスワードとともにＩＣカード読み書き機１１０に送信する。

【００６４】図５に示したように、この送信データは、カード用パスワードに、ワンタイム・パスワードおよび乱数からなる暗号用データを連結することによって構成される。

【００６５】ＩＣカード１００の暗号化機能部１０４は、ＩＣカード読み書き機１１０を介して、暗号用データを受信する。そして、このカード用パスワードを、カード用パスワード格納領域１０２から読み出したカード用パスワードと比較する。そして、両者が一致する場合には、図６に示すようなデータを生成する。

【００６６】図６に示したように、このデータは、開始コード、利用者ＩＤ、暗号用データおよび終了コードを連結することによって構成される。ここで、このデータの総バイト数は、秘密鍵のバイト数の整数倍にする必要がある。秘密鍵を８バイト長、利用者ＩＤを１０バイト長、暗号用データを１６バイト長とした場合、開始コードと終了コードとの和は例えば６バイトとすればよい。例えば、開始コードを５バイト長（例えば１６進数の４ＢＢＢＢＢＡ）とし、終了コードを１バイト長（例えば１６進数のＢＣ）とすればよい。

【００６７】続いて、暗号化機能部１０４は、秘密鍵格納領域１０３から秘密鍵を読み出し、この秘密鍵で上述のデータ（図６参照）を暗号化することによりカード暗号文を生成する。ここで、秘密鍵としては、例えばＤＥＳ方式のＣＢＣモードを使用することができる。その後、暗号化機能部１０４は、このカード暗号文をカード読み書き機１１０に出力する。

【００６８】通信端末機１２０の暗号化要求機能部１２５は、カード読み書き機１１０からカード暗号文を受信して、認証要求機能部１２６に転送する。

【００６９】認証要求機能部１２６は、暗号化要求機能部１２５から受信したカード暗号文を通信網１３０に出

力する。

【００７０】通信サーバ１４０の認証機能部１４８は、通信網１３０からカード暗号文を受信し、このカード暗号文をカード暗号文検証機能部１４６に転送する。

【００７１】カード暗号文検証機能部１４６は、秘密鍵格納領域１４２から秘密鍵を読み出し、この秘密鍵でカード暗号文を復号化することにより、図６に示したようなデータを得る。そして、開始コード（図６では１６進数の４ＢＢＢＢＢＢＡ）および終了コード（図６では１６進数のＢＣ）が含まれているか否かをチェックする。そして、開始コードおよび終了コードが含まれていた場合には、このデータから利用者ＩＤを抽出し、この利用者ＩＤに対応するＩＣカード有効／無効情報をＩＣカード表１４４から読み出して、ＩＣカードの有効／無効をチェックする。ここで、ＩＣカードが有効であった場合には、乱数の値を、チャレンジ生成機能部１４５が送信したチャレンジに含まれていた乱数の値と比較する。そして、両者が一致した場合には、ワンタイム・パスワードを出力する。一方、ＩＣカードが無効であった場合や乱数が一致しなかった場合は、所定の異常処理を行って回線を切断する。

【００７２】パスワード検証機能部１４７は、認証機能部１４８を介してカード暗号文検証機能部１４６からワンタイム・パスワード（ここではP_nとする）を入力する。そして、一方向関数$P_{n-1}=F(P_n)$を演算することによって前回の認証で使用されたワンタイム・パスワードP_{n-1}を算出した後、このワンタイム・パスワードP_{n-1}を端末機表１４３から読みだしたワンタイム・パスワードと比較し、両者が一致する場合に、カード暗号文検証機能部１４６が取得したワンタイム・パスワードP_{n-1}を端末機表１４３に格納するとともに、この端末機表１４３に記憶されているパスワード番号の値を「１」だけ増加させる。その後、認証機能部１４８から認証要求機能部１２６に認証結果が送信され、通信サーバ１４０と通信端末機１２０との間でログインのための処理が行われる。一方、これらのワンタイム・パスワードが一致しなかった場合には、所定の異常処理を行って回線を切断する。

【００７３】このように、この実施の形態によれば、使用者が自分でワンタイム・パスワードを算出する必要がないので、接続時の操作が簡単になり、パスワード生成機を携帯する必要もない。

【００７４】また、カード用パスワードは通信端末機１２０を介して通信サーバ１４０に送信されないので、このカード用パスワードを外部から不正に読み出すことはできず、従って、他人が自分でワンタイム・パスワードを生成して不正使用を行うことは不可能である。

【００７５】さらに、通信サーバが利用者の認証と通信端末機１２０の認証とを同時に行うことができる。

【００７６】なお、ＩＣカード１００の各格納領域１０１～１０３および通信端末機１２０の各格納領域１２１，１２２としては、他人の不正なデータの読み出しを困難にすることができるような不揮発性メモリを使用することが望ましい。

【００７７】

【発明の効果】以上詳細に説明したように、この発明に係る利用者カード、通信端末機、通信サーバ、通信システム、および、通信システムの利用者認証方法によれば、利用者の操作が簡単で、且つ、利用者と通信端末機の認証とを両方同時に行うことができる。

【図面の簡単な説明】

【図１】実施の形態に係る通信システムの全体構成を概略的に示すブロック図である。

【図２】実施の形態に係る利用者カードの内部構成を概略的に示すブロック図である。

【図３】実施の形態に係る通信端末機の内部構成を概略的に示すブロック図である。

【図４】実施の形態に係る通信サーバの内部構成を概略的に示すブロック図である。

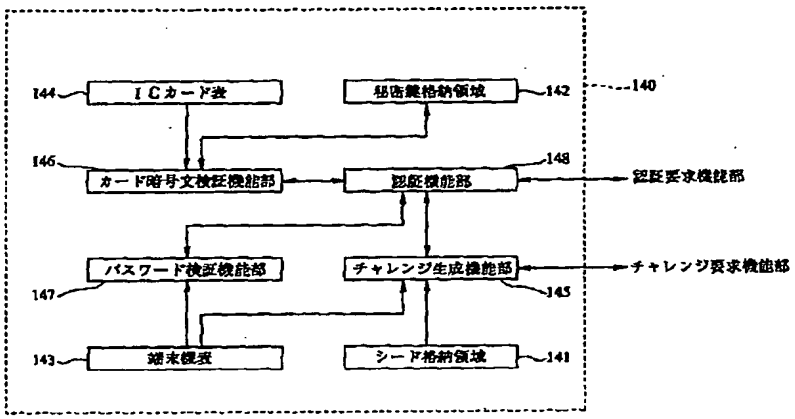
【図５】実施の形態で使用するデータの構成を示す概念図である。

【図６】実施の形態で使用するデータの構成を示す概念図である。

【符号の説明】

１００　ＩＣカード
１０１　利用者ＩＤ格納領域
１０２　カード用パスワード格納領域
１０３　秘密鍵格納領域
１０４　暗号化機能部
１１０　カード読み書き機
１２０　通信端末機
１２１　端末機ＩＤ格納領域
１２２　端末パスワード格納領域
１２３　チャレンジ要求機能部
１３０　通信網
１４０　通信サーバ
１４１　シード格納領域
１４２　秘密鍵格納領域
１４３　端末機表
１４４　ＩＣカード表
１４５　チャレンジ生成機能部
１４６　カード暗号文検証機能部
１４７　パスワード検証機能部
１４８　認証機能部

【図４】



通信サーバの内部構成図

フロントページの続き

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０９Ｃ	1/00	６６０	Ｇ０６Ｋ	19/00	Ｐ
Ｈ０４Ｌ	9/10		Ｈ０４Ｌ	9/00	６２１Ａ
	9/32				６７３Ａ
					６７３Ｂ
					６７３Ｅ